AMENDMENTS TO THE CLAIMS

Please amend claims 1, 3-14, and 16-30 as indicated among the following complete set of pending claims:

Claim 1. (Currently Amended) A multimedia contents protecting system for preventing multimedia contents, which are sent to an application program running on a client system, from leaking without permission through the use of an information providing system and the client system, the information providing system and the client system each having a Central Processing Unit (CPU), a volatile storage (memory), a non-volatile storage (hard disk) and an input/output device (keyboard, monitor, etc.), and being connected to each other through wired or wireless internal communication means or means for communicating with an external network, comprising:

the information providing system comprising,

encryption means (110) for encrypting original contents using one or more encryption keys and generating ~~a content~~ an encrypted contents package (121),

provision means (120) for holding the encrypted ~~content~~ contents package (121) and providing the encrypted ~~content~~ contents package (121) to users on line, and

a Digital Rights Management (DRM) server (130) for managing generation of the encryption keys and performing various authentication operations; and

the client system comprising,

filtering means located between ~~the~~ an application program (144) on a higher layer and a device driver on a lower layer for ~~hooking and converting a messages and a data packet~~ repeating a process of hooking data packet of the encrypted contents package (121) with messages between the application program and the device driver, converting the data packet to a format corresponding to decryption, decrypting ~~an~~ the encrypted data packet using one or more decryption keys, and sending the decrypted data packet to the application program,

control means for starting and terminating the application program and controlling the filtering means, and

an application program (144) for receiving the contents from the filtering means and playing the contents.

Claim 2. (Original) The multimedia contents protecting system as set forth in claim 1, wherein the encryption means (110) is a contents packager (112) that receives the encryption keys generated by the DRM server (130) and encrypts the contents.

Claim 3. (Currently Amended) The multimedia contents protecting system as set forth in claim 1, wherein the provision means (120) is a contents server (122) to which the ~~content~~ contents package (121) encrypted by the encryption means (110) is uploaded, and the contents server (122) is a streaming server (122a) that provides ~~actual streaming~~ the encrypted contents in a streaming manner, a Web server (122b) that allows the encrypted contents to be selected or ~~provides~~ being provided to a download service, or a File Transfer Protocol (FTP) server.

Claim 4. (Currently Amended) The multimedia contents protecting system as set forth in claim 1, wherein the DRM server (130) comprises:

a DRM server DataBase (DB) (131) for storing various data including contents ~~content~~ information ~~of the DRM server (130)~~, the encryption keys, user information and application program information of the DRM server (130);

a DRM server component (132) for ~~managing~~ controlling management of generation of the encryption keys and issuance of licenses;

a DRM license issuer (133) for issuing an encrypted license package in response to a request ~~of the DRM controller (141)~~ from the control means of the client system; and

a DRM administrator (134) for performing various setting and administration of the DRM server.

Claim 5. (Currently Amended) The multimedia contents protecting system as set forth in claim 1, wherein the information providing system further ~~comprising~~ comprises connecting means for enabling a connection to a billing server (150) or payment gateway server (160) to bill users for pay services.

Claim 6. (Currently Amended) The multimedia contents protecting system as set forth in claim 1, wherein the filtering means performs a filtering operation in kernel mode in response to an instruction of the control means, and ~~is~~ comprises a network filter driver (404) to which a network driver (403) is connected, or file filter driver (407) that converts and restores a file offset and a file length message requested by the application program (144) ~~from~~ with respect to the file system (405).

Claim 7. (Currently Amended) The multimedia contents protecting system as set forth in claim 1, wherein the control means is a DRM controller (141) that is automatically activated to initiate the application program (144) when a user selects contents in ~~a Web page~~ the provision means (120) in the case of a streaming manner or when a user issues a command to open contents downloaded to ~~a hard disk~~ a non-volatile storage in the case of a downloading manner, accesses the DRM server (130)~~, allows~~ to allow the contents and the user to be authenticated and receive the license package (143) including ~~one or more decryption keys~~ decryption key, terminates the filtering operation depending on ~~terminating~~ termination of the application program (144), and controls the filtering means.

Claim 8. (Currently Amended) The multimedia contents protecting system as set forth in claim 1, wherein the application program (144) is not a dedicated viewer program having a function of decrypting the contents package, but a general application program capable of playing ~~contents of a content package form~~ data in format of the contents package.

Claim 9. (Currently Amended) The multimedia contents protecting system as set forth in ~~claim 6~~ claim 1, wherein the client system further comprises storage means that revises or edits contents that the application program (144) have decrypted and read in, and encrypts and stores the revised or edited contents, and the ~~network filter driver (404 or file filter driver (407)~~ filtering means further comprises an encryption means for encrypting the contents.

Claim 10. (Currently Amended) The multimedia contents protecting system as set forth in ~~claim 6~~ claim 1, wherein the ~~network filter driver (404 or file filter driver (407)~~ filtering means is ~~situated~~ located on an uppermost ~~one~~ end of layers of the device driver ~~layers~~ in a direction toward the application program (144).

Claim 11. (Currently Amended) The multimedia contents protecting system as set forth in claim 6, wherein the network filter driver (404) uses a Transmission Control Protocol (TCP), or User Diagram Protocol (UDP) ~~additionally~~ further having a function of correcting received data.

Claim 12. (Currently Amended) The multimedia contents protecting system as set forth in any of claims 1 to 11, wherein ~~continuous content packets are sent and played in the case of a streaming manner, further comprising storage means for allowing content packets to be downloaded to the client system (140) and to be stored therein~~ the client system (140) further comprises storage means for storing a continuous contents packets which are downloaded

during transferring and playing the continuous contents packets in the case of a streaming manner.

Claim 13. (Currently Amended) The multimedia contents protecting system as set forth in any of ~~claims 1 to 12~~ claims 1 to 11, wherein the ~~multimedia contents are sent~~ encrypted contents package (121) is transferred in one of a Video On Demand (VOD) streaming manner, a real-time live streaming manner, a complete downloading manner and a Hyper Text Transfer Protocol (HTTP) streaming manner, or off line in a storage medium, such as Compact Disk (CD) or Digital Versatile Disk (DVD).

Claim 14. (Currently Amended) The multimedia contents protecting system as set forth in claim 13, wherein the transferring is performed in a real-time live streaming manner, and the original contents are input through a multimedia receiving device and a encoding system, and the encrypted contents are transferred to the provision means (120) through the network driver of the encoding system, and the encoding system further ~~comprising~~ comprises a network filter driver disposed upstream of the network driver ~~of an encoding system~~ for ~~performing~~ generating the encrypted contents through real-time hooking and encryption ~~before the real-time live contents are sent to an external streaming server in the case of a real-time live streaming manner in which the sending of the multimedia contents are performed through a multimedia receiving device and the encoding system~~ with respect to the original contents.

Claim 15. (Original) The multimedia contents protecting system as set forth in claim 1, wherein the encrypted contents package (142) comprises at least a data object portion that are encrypted contents (142a) and a header object portion that are non-encrypted meta data (142b).

Claim 16. (Currently Amended) The multimedia contents protecting system as set forth in claim 15, wherein ~~a DRM package header of the encrypted content package (142) is recorded in the header object of a multimedia content file form~~ the header object portion comprises a DRM package header for recording information on contents and encryption of the encrypted contents package (142).

Claim 17. (Currently Amended) The multimedia contents protecting system as set forth in claim 16, wherein the DRM package header includes one or more information of a version number, a contents Uniform Resource Identifier (URI) length, a contents type length, a contents URI, a contents type, a header length, a data length, an encryption method, a rights issuer Uniform Resource ~~Identifier~~ Locator (URL), a contents name, a contents description, a contents vendor, an icon URI, a digital signature, and a contents server URL.

Claim 18. (Currently Amended) The multimedia contents protecting system as set forth in claim 15, wherein the data object ~~that is the encrypted contents (142a)~~ portion is fully encrypted or partially encrypted in ~~one or more predetermined frames~~ predetermined portion on frame basis.

Claim 19. (Currently Amended) The multimedia contents protecting system as set forth in ~~claim 15~~ claim 1, wherein the client system further comprises ~~storage~~ storing means for storing the encrypted contents package to a non-volatile storage means.

Claim 20. (Currently Amended) The multimedia contents protecting system as set forth in claim 1, wherein the control means receives encrypted license package (143) from the DRM server (130) in response to a request for authentication, and the encrypted license package (143) ~~sent to the client system in response to a request of the user for authentication~~ comprises:

a decryption key (143a) ~~for performing decryption~~ portion for being used in decryption of the encrypted contents package; and

usage ~~rights~~ authority information (143b) portion including at least a count of use and a period of use of the contents and terminal restriction information.

Claim 21. (Currently Amended) A multimedia contents protecting method of preventing multimedia contents, which are sent to an application program running on a client system, from leaking without permission through the use of an information providing system and the client system, the information providing system and the client system each having a CPU, a volatile storage (memory), a non-volatile storage (hard disk) and an input/output device (keyboard, monitor, etc.), and being connected to each other through wired or wireless internal communication means or means for communicating with an external network, comprising:

~~the~~ an encrypting and uploading step of ~~converting original contents (111) into an encrypted content package (121) using one or more encryption keys of a DRM server and uploading the encrypted content package (121) to a content server (122)~~ an encrypted contents package (121) converted from an original contents (111) using encryption keys being uploaded to the information providing system through the communication means;

~~the~~ an initiating and connecting step of ~~connecting the client system to the content server (122) and initiating streaming or downloading service by selecting contents in a Web server (122b) or FTP server~~ the client system being connected to the information providing system to initiate streaming or downloading service by selection of encrypted contents package (121) in the information providing system using the input device of the client system;

~~the~~ a decrypting and playing step of ~~decrypting and playing content data through an application program (144) in response to a signal from a player during sending in the case of a streaming manner, or after downloading in the case of a downloading manner~~ the client system making the encrypted data played through the output device by the application program (144) ,by a filtering operation repeating a process of hooking data packet of the encrypted contents

package (121) with messages between the application program (144) on a higher layer and the device driver on a lower layer, converting the data packet to a format corresponding to decryption, decrypting the encrypted data packet using one or more decryption keys, and sending the decrypted data packet to the application program, during transferring in the case of a streaming manner, or in response to a play signal after downloading in the case of a downloading manner; and

~~the~~ a terminating step of the client system terminating the operation of the application program (144) and the filtering operation and disconnecting ~~the client system from the content server (122)~~ connection to the information providing system in the case of a streaming manner, when ~~a DRM controller (141) detects~~ a termination command of the application program (144) is detected.

Claim 22. (Currently Amended) The multimedia contents protecting method as set forth in claim 21, wherein the information providing system comprises

encryption means (110) for encrypting original contents using one or more encryption keys and generating a encrypted contents package (121),

provision means (120) for holding the encrypted contents package (121) and providing the encrypted contents package (121) to users on line, and

a Digital Rights Management (DRM) server (130) for managing generation of the encryption keys and performing various authentication operations; and

the encrypting and uploading step comprises:

~~the~~ a step ~~(S21 and S22)~~ of the ~~content packager (112)~~ encryption means (110) requesting (S21) and obtaining (S22) an authentication ~~from~~ with respect to the DRM server (130);

~~the~~ a step ~~(S23 and S24)~~ of the ~~content packager (112)~~ encryption means (110) requesting (S23) and obtaining (S24) one or more encryption keys ~~from~~ with respect to the DRM server (130);

~~the~~ a step of the ~~content packager (112)~~ encryption means (110) encrypting an original contents using the encryption keys;

~~the~~ a step ~~(S25 and S26)~~ of the ~~content packager (112)~~ encryption means (110) requesting (S25) and obtaining (S26) an authentication ~~from the content server (122)~~ with respect to the provision means (120); and

~~the~~ a step ~~(S27)~~ of the ~~content packager (112)~~ encryption means (110) sending (S27) the encrypted contents package (121) to the ~~content server (122)~~ provision means (120).

Claim 23. (Currently Amended) The multimedia contents protecting method as set forth in claim 21, wherein

the information providing system comprises

encryption means (110) for encrypting original contents using one or more encryption keys and generating a encrypted contents package (121),

provision means (120) for holding the encrypted contents package (121) and providing the encrypted contents package (121) to users on line, and

a Digital Rights Management (DRM) server (130) for managing generation of the encryption keys and performing various authentication operations; and

the initiating and connecting step comprises:

~~the~~ a step ~~(S31)~~ of the ~~Webserver (122b) or FTP server~~ provision means (120) sending (S31) contents identification information and user identification information to the ~~DRM controller (141) if the application program (144) is commanded to retrieve contents after downloading the contents~~ client system, when an open command of the application program (144) is issued with respect to the encrypted contents package (121) after download completed

in the case of a downloading manner, or ~~if~~ when the contents in the provision means (120) are selected ~~on a Web page~~ in the case of a streaming manner;

~~the~~ a step ~~(S32 and S33)~~ of the ~~DRM controller (141)~~ client system requesting (S32) contents and user authentication ~~from the DRM server (130)~~ and receiving (S33) license authentication including [[a]] one or more decryption ~~key~~ keys and ~~user~~ usage authority information with respect to the DRM server (130);

~~the~~ a step ~~(S34)~~ of the ~~DRM controller (141)~~ client system sending (S34) to the application program (144), an URL of the ~~content server (122)~~ provision means (120) in the case of a streaming manner, a position of ~~a hard disk~~ the non-volatile storage device where the contents are stored in the case of a complete downloading manner, and both the URL of the ~~content server (122)~~ provision means (120) and the position of the ~~hard disk~~ non-volatile storage device in the case of a HTTP streaming manner, after initiating the application program (144); and

~~the~~ a step ~~(S35)~~ of the ~~DRM controller (141)~~ client system requesting (S35) the contents data ~~from the content server (122)~~, to the provision means (120) in the case of a streaming manner, to the file system in the case of a downloading manner, and to both the ~~content server (122)~~ provision means (120) and the file system in the case of a HTTP streaming manner.

Claim 24. (Currently Amended) The multimedia contents protecting method as set forth in claim 23, further comprising:

~~the~~ a connection preparing step of ~~performing~~ examination of a handler and registration of a process being performed after the initiation of the application program (144) ~~is initiated~~ by the client system; and

~~the~~ a connecting step of ~~performing next~~ registration of a next process and ascertainment and storing of a remote port being performed.

Claim 25. (Currently Amended) The multimedia contents protecting method as set forth in claim 24, wherein the client system comprises filtering means located between an application program (144) on a higher layer and a device driver on a lower layer for performing a filtering operation repeating a process of hooking data packet of the encrypted contents package (121) with messages between the application program and the device driver, converting the data packet to a format corresponding to decryption, decrypting the encrypted data packet using one or more decryption keys, and sending the decrypted data packet to the application program, and

the connection preparing step comprises:

~~the~~ a step of ~~starting and temporarily stopping~~ the application program (144) being temporarily stopped after initiation;

~~the~~ a step of ~~the DRM controller (141) determining whether the handler is zero~~ the handler being determined whether zero or not by ~~hooking~~ a message between the application program (144) and the ~~network driver or file system using~~ device driver hooked by the filtering means;

~~the~~ a step of ~~deleting an address handle to cancel the connection and sending a messge to the network driver or file system if the handler is zero, and determining whether a process is registered in the filtering means if the handler is not zero~~ the message being sent to the device driver after deletion of an address handle to cancel connection if the handler is zero, and a process being determined whether registered in the filtering means or not if the handler is not zero;

~~the~~ a step of ~~sending a message to the network driver or file system if the process is not registered in the filtering means, and registering an address handle, setting a my event handler, storing a local port and sending a changed message to the network driver or file system if the process is registered in the filtering means~~ the message being sent to the device driver as it is if the process is not registered, and a changed message being sent to the device driver after an

address handle being registered, my event handler being set, and a local port being stored if the process is registered; and

~~the~~ a step of the application program (144) receiving a ready message from the ~~network~~ device driver ~~or file system through the~~ by sending the message.

Claim 26. (Currently Amended) The multimedia contents protecting method as set forth in claim 24, wherein

the client system comprises filtering means located between an application program (144) on a higher layer and a device driver on a lower layer for performing a filtering operation repeating a process of hooking data packet of the encrypted contents package (121) with messages between the application program and the device driver, converting the data packet to a format corresponding to decryption, decrypting the encrypted data packet using one or more decryption keys, and sending the decrypted data packet to the application program, and

the connecting step comprises:

~~the~~ a step of ~~the filtering means hooking a message between the application program (144) and the network driver or file system and determining whether the process is registered in the filtering means~~ a process being determined (801) whether registered in the filtering means or not by a message between the application program (144) and the device driver hooked by the filtering means;

~~the~~ a step of ~~sending the message the network driver or file system if the process is not registered in the filtering means, and determining whether a remote port has a predetermined number if the process is registered in the filtering means~~ the message being sent to the device driver as it is if the process is not registered, and the number of the remote port being determined whether a predetermined number or not if the process is registered; and

~~the~~ a step of ~~sending the message to the network driver or file system if the remote port does not have the predetermined number, and sending the message to the network driver or file~~

~~system after storing a remote port number in an address handle structure having a local port connected to the remote port if the remote port has the predetermined number~~ the message being sent to the device driver as it is if the number of the remote port is not a predetermined number, the message being sent to the device driver as it is after the number of the remote port is stored in an address handle structure having local port connected to the remote port if the number of the remote port is a predetermined number.

Claim 27. (Currently Amended) The multimedia contents protecting method as set forth in claim 21, wherein

the encrypting and playing step comprises:

~~the~~ a step ~~(901)~~ of ~~a storage in the case of downloading, and the content server (122) in the case of streaming~~ the data packet being sent periodically ~~sending a data packet~~ to the application program (144) along with control information, from the non-volatile storage device in the case of downloading manner, or from the information providing system in the case of streaming manner;

~~the~~ a step ~~(403)~~ of ~~hooking~~ the data packet being hooked (403) by ~~using~~ the filtering ~~means~~ operation;

~~the~~ a step of ~~determining whether a remote port has~~ the number of a remote port being determined whether a predetermined number ~~in a state in which the~~ or not after my event handler is activated;

~~the~~ a step ~~(902)~~ of ~~sending the data packet to the application program (144) if the remote port does not have the predetermined number, and decrypting the data packet and sending the decrypted data packet to the application program (144) if the remote port has the predetermined number~~ the data packet being sent to the application program (144) as it is if the number of the remote port is not a predetermined number, the data packet being sent to the application

program after decryption (905) by the decryption keys if the number of the remote port is a predetermined number; and

~~the~~ a step of ~~playing the data packet~~ the multimedia contents being played by repeating the above steps.

Claim 28. (Currently Amended) The multimedia contents protecting method as set forth in claim 27, further comprising:

~~the~~ a step of ~~determining~~ the encrypted contents being determined whether ~~the data packet is~~ to be stored in the ~~hard disk~~ non-volatile storage device or not before ~~being decrypted~~ the decryption (905); and

~~the~~ a step of ~~decrypting the data packet~~ the encrypted contents being decrypted (905) as it is if the ~~data packet is not stored in the hard disk~~ choice is no storing in the non-volatile storage device, and ~~decrypting the data packet after being stored in the hard disk if the data packet is not stored in the hard disk~~ the encrypted contents being decrypted (905) after being stored in the non-volatile storage device if the choice is storing in the non-volatile storage device.

29. (Currently Amended) The multimedia contents protecting method as set forth in claim 21, wherein the terminating step comprises:

the step of ~~the DRM controller (141) detecting a termination message of the application program (144) every cycle in which the content data packet is decrypted and played~~ a termination message of the application program (144) being monitored in every cycle wherein the contents data packet is decrypted and played; and

the step of returning to the decrypting and playing step if the termination message is not detected, and disconnecting ~~the client system from the content server (122)~~ connection to the information providing system or ~~hard disk by terminating~~ the non-volatile storage device after

termination of the application program (144) and ~~deleting~~ deletion of the address handle if the termination message is detected.

Claim 30. (Currently Amended) A computer-readable storage medium for storing a computer-executable multimedia contents protecting method of preventing multimedia contents, which are sent to an application program running on a client system, from leaking without permission through the use of an information providing system and the client system, the information providing system and the client system each having a CPU, a volatile storage (memory), a non-volatile storage (hard disk) and an input/output device (keyboard, monitor, etc.), and being connected to each other through wired or wireless internal communication means or means for communicating with an external network, the multimedia contents protecting method comprising:

~~the~~ an encrypting and uploading step of ~~converting original contents (111) into an encrypted content package (121) using one or more encryption keys of a DRM server and uploading the encrypted content package (121) to a content server (122)~~ an encrypted contents package (121) converted from an original contents (111) using encryption keys being uploaded to the information providing system through the communication means;

~~the~~ an initiating and connecting step of ~~connecting the client system to the content server (122) and initiating streaming or downloading service by a user selecting contents in a Web server (122b) or FTP server~~ the client system being connected to the information providing system to initiate streaming or downloading service by selection of encrypted contents package (121) in the information providing system using the input device of the client system;

~~the~~ a decrypting and playing step of ~~decrypting and playing content data through an application program (144) in response to a signal from a player during sending in the case of a streaming manner, or after downloading in the case of downloading manner~~ the client system making the encrypted data played through the output device by the application program (144)

,by a filtering operation repeating a process of hooking data packet of the encrypted contents package (121) with messages between the application program (144) on a higher layer and the device driver on a lower layer, converting the data packet to a format corresponding to decryption, decrypting the encrypted data packet using one or more decryption keys, and sending the decrypted data packet to the application program, during transferring in the case of a streaming manner, or in response to a play signal after downloading in the case of a downloading manner; and

~~the~~ a terminating step of the client system terminating ~~an~~ the operation of the application program (144) and [[a]] the filtering operation and disconnecting ~~the client system from the content server (122)~~ connection to the information providing system in the case of a streaming manner, when ~~a DRM controller (141) detects~~ a termination command of the application program (144) is detected.